REMARKS

The application has been amended and is believed to be in condition for allowance.

Claim 1 is the only independent claim.

Claims 1 and 9 have been amended by adding the following characteristics:

- the authentication password (MPAUT) is built by applying a user known key to the voice message; this characteristic is supported by claim 4 as filed, by page 6, lines 14-20 of the application, and by page 13, lines 15-21 of the application.

- the authentication password (MPAUT) is directly built by the user; as disclosed in page 4, lines 17-19 of the application, that means that the user is directly doing an intellectual step and does not require any special identification computer device to built the authentication password (MPAUT); this characteristic is supported by the application, for example page 8, lines 17-20.

No new matter is entered by way of these amendments.

CLAIM REJECTIONS - 35 USC §112

The claims were rejected as indefinite under Section 112, second paragraph. The Official Action stated that it was not clear what the structures corresponding to the means-plus-function limitations are in the specification.

Responsively, reference numbers have been included in claims 1 and 9-11 in order to illustrate the "means plus function" disclosed in claims 1 and 9-11. Withdrawal of the indefiniteness rejection is therefore solicited.

CLAIM REJECTIONS 35 USC §103 RATAYCZAK

The Official Action rejects claims 1-3, 5, 9-10, and 12 of the application as being unpatentable over RATAYCZAK (US Patent 6,259,909).

In the realization mode illustrated in Figure 5 of RATAYCZAK, a protocol of authenticating a client site user comprises a sequence S51 of receiving and processing identification data ("first code word" column 6, lines 59-64 of RATAYCZAK) from the first communication device C1, and a sequence S52 of transmitting a message ("second code word" column 7, lines 1-5 of RATAYCZAK) from the access device to the second communication device C2 through a second communication network.

In a further step S53, the second code word can be transmitted from the second communication device C2 to the first communication device C1, for example by a read out operation from the first communication device C1 and an input operation at the second communication device C2 (column 7, lines 6-13 of RATAYCZAK).

In a still further step S54, the second code word is transmitted from the first communication device to access device

A and is checked there for correctness (column 7, lines 14-19 of RATAYCZAK).

RATAYCZAK differs from claim 1 of the application, in that according to the claim, the message is a voice message.

In step S52 of RATAYCZAK, the "second code word" transmitted from the access device to the second communication device C2 is not a voice message.

According to claim 1 of the application, a user known key is applied by the user to the voice message (MPA) in order to build the authentication password (MPAUT). This is not taught by RATAYCZAK. Thus, the authentication password (MPAUT) is different from the voice message (MPA). Even if RATAYCZAK were modified to include a voice message, this recitation would not be satisfied.

In step S53 of RATAYCZAK, the second code word is just transmitted from the second communication device C2 to the first communication device C1 without modifications. This means that the message sent by the access device A in step S52 is the same as the message received by the access device A in step S54. Accordingly, RATAYCZAK would not teach or suggest the invention as now claimed.

For these reasons, claim 1 is believed to be patentable over RATAYCZAK.

Claim 9 recites the same subject matter as claim 1, and claim 12 is directed to an application for utilizing the process

of claim 1. The dependent claims are believed patentable at least for depending from an allowable claim.

CLAIM REJECTIONS 35 USC §103 RATAYCZAK, GUTHRIE, KELLY

I. The Examiner rejects claims 4 and 6 of the application as being unpatentable over RATAYCZAK in view of GUTHRIE (US 6,161,185).

GUTHRIE discloses (see Figure 4 of GUTHRIE) a method for generating an authentication password (or "response"), by applying a key on a message (or "challenge") sent by a server.

According to GUTHRIE, the authentication password is generated by a SADB calculator, this calculator implementing a SHA algorithm (see column 2, line 57, and column 5, line 43 to column 7, line 9 of GUTHRIE).

Thus, GUTHRIE does not disclose that the authentication password (MPAUT) is directly built by a human user knowing a key and directly using this key. GUTHRIE does not even suggest that the authentication password (MPAUT) could be directly built by the user, because a SHA algorithm is too complicated to be implemented by a human brain.

Therefore, any combination of RATAYCZAK and GUTHRIE would comprise a calculator to build an authentication password from a message sent by a server. Such a combination would not satisfy the pending claims.

Additionally, note that the claimed process and system according the application has many advantages compared to any combination of RATAYCZAK and GUTHRIE:

a user of a process or system according to the application is more free, because he does not need any personal calculator, as disclosed on page 4, lines 17-19 of the application,

a process or system according the application is more secured, because no personal calculator of a user can be stolen, and

a process or system according the application is more secured because, as a user is directly building the authentication password, this user can intentionally build a wrong authentication password if he is threaten by a criminal.

For these reasons, claim 1, as well as claims 4 and 6 and the remaining dependent claims, are believed to be non-obvious and thus patentable over RATAYCZAK in view of GUTHRIE.

II. The Examiner rejects claims 7 and 11 of the application as being unpatentable over RATAYCZAK in view of KELLY (US 5,636,280).

KELLY does not disclose a generation of an authentication password (MPAUT) directly built by a human user knowing a key and directly using this key.

For the reasons previously disclosed, claims 1 and 9, as well as claims 7 and 11 and the other dependent claims, are believed to be patentable over RATAYCZAK in view of KELLY.

III. The Examiner rejects claim 8 of the application as being unpatentable over RATAYCZAK in view of KELLY and in further view of GUTHRIE.

As discussed above, neither GUTHRIE nor KELLY discloses a generation of an authentication password (MPAUT) directly built by a human user knowing a key and directly using this key. For the reasons previously disclosed, claim 1, as well as claim 8 and the other dependent claims, are believed to be patentable over RATAYCZAK further in view of KELLY and GUTHRIE.

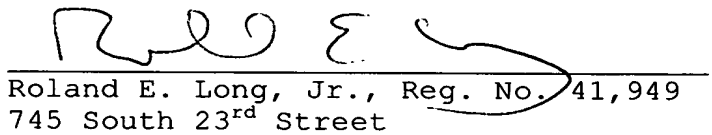
In conclusion, all the claims are believed patentable as the references, taken individually or in combination, do not teach or suggest all the claimed features of the invention. Withdrawal of all of the obviousness rejections and allowance of all the claims are therefore respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any

overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



Roland E. Long, Jr., Reg. No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573

REL/lk